

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

26.07.2004

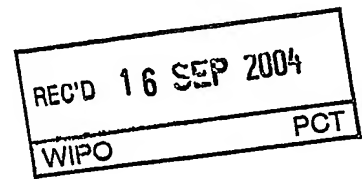
別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日  
Date of Application: 2003年 6月20日

出 願 番 号  
Application Number: 特願2003-176568  
[ST. 10/C]: [JP2003-176568]

出 願 人  
Applicant(s): 日本電信電話株式会社



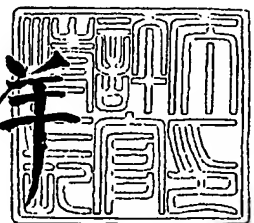
BEST AVAILABLE COPY

PRIORITY DOCUMENT  
SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH  
RULE 17.1(a) OR (b)

2004年 9月 2日

特許庁長官  
Commissioner,  
Japan Patent Office

小 川 洋



【書類名】 特許願  
【整理番号】 NTTH155517  
【あて先】 特許庁長官殿  
【国際特許分類】 H04L 12/00  
【発明者】

【住所又は居所】 東京都千代田区大手町二丁目 3 番 1 号 日本電信電話株式会社内

【氏名】 小野 久美子

【発明者】

【住所又は居所】 東京都千代田区大手町二丁目 3 番 1 号 日本電信電話株式会社内

【氏名】 立元 慎也

【発明者】

【住所又は居所】 東京都千代田区大手町二丁目 3 番 1 号 日本電信電話株式会社内

【氏名】 坂谷 精一

【特許出願人】

【識別番号】 000004226

【氏名又は名称】 日本電信電話株式会社

【代理人】

【識別番号】 100077274

【弁理士】

【氏名又は名称】 磯村 雅俊

【電話番号】 03-3348-5035

【選任した代理人】

【識別番号】 100102587

【弁理士】

【氏名又は名称】 渡邊 昌幸

【電話番号】 03-3348-5035

【手数料の表示】

【予納台帳番号】 013402

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9701395

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 セッション制御サーバ、通信装置、通信システムおよび通信方法、ならびにそのプログラムと記録媒体

【特許請求の範囲】

【請求項 1】 ネットワークを介してセッション制御サーバと通信可能に接続され、1 以上の前記セッション制御サーバを経由した他の通信装置との間で信号送受信を行うことで、該通信装置とのセッションを確立する通信装置において、

送信信号の守秘性を保持するために暗号化した情報を送信する際に、情報暗号化のための第一の暗号化鍵を生成する手段と、

該第一の暗号化鍵を用いて情報を暗号化する手段と、

該第一の暗号化鍵を任意の第二の暗号化鍵で暗号化する暗号化鍵暗号化手段と、

任意の第二の暗号化鍵で暗号化した第一の暗号化鍵を添付した、該第一の暗号化鍵で暗号化された情報を含む信号を送信する手段とを備え、

前記暗号化鍵暗号化手段は、該第一の暗号化鍵を、送信先の通信装置または 1 以上の該セッション制御サーバの各々が保有する第二の暗号化鍵を用いて暗号化し、

前記送信手段は、暗号化された該第一の暗号化鍵と、該第一の暗号化鍵により暗号化された情報と、該セッション制御サーバに対する該情報の復号化要求指示を送信することを特徴とする通信装置。

【請求項 2】 ネットワークを介して複数の通信装置と他のセッション制御サーバと通信可能に接続され、発信側の通信装置あるいは他のセッション制御サーバから送信された信号を受信し、受信した信号を着信側の通信装置あるいは他のセッション制御サーバに送信することで、該発信側の通信装置と該着信側の通信装置のセッションを確立させるセッション制御サーバにおいて、

暗号化された第一の暗号化鍵を添付し、かつ該第一の暗号化鍵で暗号化された情報を含む信号を受信する手段と、

該第一の暗号化鍵を復号化する手段と、  
復号化した該第一の暗号化鍵を用いて、情報を復号化する手段とを備え、  
前記受信手段が信号を受信すると、前記復号化手段は、復号化要求の有無、復号化対象の情報を判断し、第二の暗号化鍵に対応した第二の復号化鍵で該第一の暗号化鍵を復号化するか、あるいは、該第二の暗号化鍵に対応した第二の復号化鍵で該第一の暗号化鍵を復号化することで、復号化要求の有無を判断することを特徴とするセッション制御サーバ。

【請求項 3】 請求項 2 記載のセッション制御サーバにおいて、  
前記第一の暗号化鍵をセッション単位に保管もしくは記憶する手段を備え、  
該第一の暗号化鍵を同一セッション内で、情報の復号化に再利用することを特徴とするセッション制御サーバ。

【請求項 4】 ネットワークを介してセッション制御サーバと通信可能に接続され、前記セッション制御サーバとの間で信号送受信を行うことで、他の通信装置とのセッションを確立する通信装置において、

暗号化した第一の暗号化鍵を添付し、かつ該第一の暗号化鍵で暗号化された情報を含む信号を受信する手段と、

該第一の暗号化鍵を復号化する手段と、  
得られた該第一の暗号化鍵により情報を復号化する手段と、  
該第一の暗号化鍵をセッション単位に保管あるいは記憶する手段と、  
該第一の暗号化鍵を用いて情報を暗号化する手段と、  
該第一の暗号化鍵で暗号化された情報を含む信号を送信する手段とを備え、  
同一セッション内の情報の暗号化および復号化に、前記第一の暗号化鍵を利用することを特徴とする着信側の通信装置。

【請求項 5】 請求項 1 記載の通信装置において、  
前記第一の暗号化鍵をセッション単位に保管あるいは記憶する手段と、  
該第一の暗号化鍵を用いて情報を暗号化する手段と、  
該第一の暗号化鍵で暗号化された情報を含む信号を送信する手段と、  
該第一の暗号化鍵で暗号化された情報を含む信号を受信する手段と、  
該第一の暗号化鍵を用いて情報を復号化する手段とを備え、

同一セッション内の情報の暗号化および復号化に、前記第一の暗号化鍵を利用することを特徴とする発信側の通信装置。

【請求項 6】 請求項 4 または 5 記載の通信装置において、  
セッション単位に管理した前記第一の暗号化鍵を、周期的に更新する手段を備え、

該周期的更新手段は、新規に該第一の暗号化鍵を生成する手段と、  
該第一の暗号化鍵を、任意の第二の暗号化鍵により暗号化する暗号化鍵暗号化手段と、

任意の第二の暗号化鍵で暗号化した該第一の暗号化鍵を添付し、かつ該第一の暗号化鍵で暗号化された情報を含む信号を送信する手段と  
からなることを特徴とする通信装置。

【請求項 7】 請求項 3 記載のセッション制御サーバにおいて、  
セッション単位に管理した前記第一の暗号化鍵を、周期的に更新する手段を備え、

該周期的更新手段は、任意の第二の暗号化鍵で暗号化した該第一の暗号化鍵を添付し、かつ該第一の暗号化鍵で暗号化された情報を含む信号を受信する手段と  
からなることを特徴とするセッション制御サーバ。

【請求項 8】 ネットワークを介して互いに通信可能に接続され、信号送受信を行うことで、セッションを確立する通信システムにおいて、

送信信号の守秘性を保持するために暗号化した情報を含む信号を送信する際に、暗号化のための第一の暗号化鍵を生成する手段と、該第一の暗号化鍵を用いて情報を暗号化する手段と、該第一の暗号化鍵を任意の第二の暗号化鍵で暗号化する暗号化鍵暗号化手段と、任意の第二の暗号化鍵で暗号化した第一の暗号化鍵を添付した、該第一の暗号化鍵で暗号化された情報を含む信号を送信する手段とを備え、前記暗号化鍵暗号化手段は、該第一の暗号化鍵を、送信先の通信装置または 1 以上の該セッション制御サーバの各々が保有する第二の暗号化鍵を用いて暗号化し、前記送信手段は、暗号化された該第一の暗号化鍵と、該第一の暗号化鍵により暗号化された情報を含む信号と、該セッション制御サーバに対する復号化要求指示を送信する第 1 の通信装置と、

暗号化した第一の暗号化鍵を添付し、かつ該第一の暗号化鍵で暗号化された情報を含む信号を受信する手段と、該第一の暗号化鍵を復号化する手段と、得られた該第一の暗号化鍵により情報を復号化する手段と、該第一の暗号化鍵をセッション単位に保管あるいは記憶する手段と、該第一の暗号化鍵を用いて情報を暗号化する手段と、該第一の暗号化鍵で暗号化された情報を含む信号を送信する手段とを備え、同一セッション内の情報の暗号化および復号化に、前記第一の暗号化鍵を利用する第2の通信装置と、

暗号化された第一の暗号化鍵を添付し、かつ該第一の暗号化鍵で暗号化された信号を受信する手段と、該第一の暗号化鍵を復号化する手段と、復号化した該第一の暗号化鍵を用いて、情報を復号化する復号化手段とを備え、前記受信手段が信号を受信すると、前記復号化手段は、復号化要求の有無を判断し、第二の暗号化鍵に対応した第二の復号化鍵で該第一の暗号化鍵を復号化するか、あるいは、該第二の暗号化鍵に対応した第二の復号化鍵で該第一の暗号化鍵を復号化することで、復号化要求の有無を判断するセッション制御サーバとを有することを特徴とした通信システム。

【請求項9】 ネットワークを介して互いに通信可能に接続され、信号送受信を行うことで、セッションを確立する通信システムにおいて、

暗号化した第一の暗号化鍵を添付し、かつ該第一の暗号化鍵で暗号化された情報を含む信号を受信する手段と、該第一の暗号化鍵を復号化する手段と、得られた該第一の暗号化鍵により情報を復号化する手段と、該第一の暗号化鍵をセッション単位に保管あるいは記憶する手段と、該第一の暗号化鍵を用いて情報を暗号化する手段と、該第一の暗号化鍵で暗号化された情報を含む信号を送信する手段とを備え、同一セッション内の情報の暗号化および復号化に、前記第一の暗号化鍵を利用する着信側の通信装置と、

請求項1に記載の各手段に加え、前記第一の暗号化鍵をセッション単位に保管あるいは記憶する手段と、該第一の暗号化鍵を用いて情報を暗号化する手段と、該第一の暗号化鍵で暗号化された情報を含む信号を送信する手段と、該第一の暗号化鍵で暗号化された情報を含む信号を受信する手段と、該第一の暗号化鍵を用いて情報を復号化する手段とを備え、同一セッション内の情報の暗号化および復

号化に、前記第一の暗号化鍵を利用する発信側の通信装置と、

請求項 2 に記載の各手段に加え、前記第一の暗号化鍵をセッション単位に保管もしくは記憶する手段を備え、該第一の暗号化鍵を同一セッション内で、情報の復号化に再利用するセッション制御サーバとを有することを特徴とした通信システム。

【請求項 10】 ネットワークを介して互いに通信可能に接続され、信号送受信を行うことで、セッションを確立する通信システムにおいて、

請求項 4 または 5 に記載の各手段に加えて、セッション単位に管理した前記第一の暗号化鍵を、周期的に更新する手段を備え、該周期的更新手段は、新規に該第一の暗号化鍵を生成する手段と、該第一の暗号化鍵を、任意の第二の暗号化鍵により暗号化する暗号化鍵暗号化手段と、任意の第二の暗号化鍵で暗号化した該第一の暗号化鍵を添付し、かつ該第一の暗号化鍵で暗号化された情報を含む信号を送信する手段とからなる通信装置と、

請求項 2 に記載の各手段に加えて、前記第一の暗号化鍵を周期的に更新する手段と、前記第一の暗号化鍵をセッション単位に保管もしくは記憶する手段を備え、該第一の暗号化鍵を同一セッション内で、情報の復号化に再利用するセッション制御サーバとを有することを特徴とした通信システム。

【請求項 11】 通信装置で生成したセッション制御信号が、信頼されるセッション制御サーバと、信頼されないセッション制御サーバ経由で他の通信装置に送信される通信方法において、

信頼されるセッション制御サーバは、該通信装置から送信された信号を受信すると、復号化判断手段により復号化要求の有無を判断し、要求があれば、暗号化鍵復号化手段により第一の暗号化鍵の復号化を行い、復号化された該第一の暗号化鍵を用いて信号復号化手段により情報を復号化し、該情報を信頼されないセッション制御サーバに送信し、該セッション制御サーバは、これを受信し、前と同一処理を施して着信側通信装置に送信し、該着信側通信装置は、受信した信号の情報が第一の暗号化鍵で暗号化されており、かつ該第一の暗号化鍵が暗号化されて添付されているときは、自身の第二の暗号化鍵に対応する第二の復号化鍵を用



いて暗号化鍵復号化手段により復号化し、第一の暗号化鍵を取得し、該第一の暗号化鍵を用いて暗号化された情報を信号復号化手段により復号化することを特徴とする通信方法。

【請求項 12】 セッション制御サーバがセッション確立中、あるいは、セッション変更中に得られた情報を元に NAT／ファイアウォール装置のフィルタリング条件を変更する通信方法において、

セッション制御サーバは、通信装置の主情報通信経路の IP アドレスとポート番号を元に、NAT／ファイアウォール装置に対してフィルタリング条件の変更を要求し、不特定 IP アドレスから特定 IP アドレスおよびポート番号宛のパケットを通過させ、その後、他の通信装置から受信した暗号化情報を第一暗号化鍵を用いて復号化し、該通信装置の主情報通信経路の IP アドレスとポート番号を元に、NAT／ファイアウォール装置に対してフィルタリング条件の変更を要求し、特定 IP アドレスから特定 IP アドレスおよびポート番号宛のパケットを通過させ、その後、通信装置からメッセージの切断信号を受信すると、NAT／ファイアウォール装置に対してフィルタリング条件の変更を要求し、指定 IP アドレスから指定 IP アドレスおよびポート番号宛のパケットを不通過とさせることを特徴とする通信方法。

【請求項 13】 セッション制御サーバがセッション確立中、あるいは、セッション変更中に得られた情報を元に、暗号化された主情報について通信記録を可能にする通信方法において、

セッション制御サーバは、通信装置の主情報通信経路の IP アドレスとポート番号を元に、NAT／ファイアウォール装置に対して、フィルタリング条件変更要求に加えて、主情報転送を指示し、該 NAT／ファイアウォール装置から主情報を受信すると、取得済みの主情報暗号化の鍵情報を用いて主情報復号化手段により復号化を行い、復号化が終了すると、復号化された状態の主情報とその鍵情報を記録することを特徴とする通信方法。

【請求項 14】 通信装置で生成したセッション制御信号が、信頼されるセッション制御サーバと、信頼されないセッション制御サーバ経由で他の通信装置に送信されるセッション制御用プログラムであって、

信頼されるセッション制御サーバのコンピュータに、該通信装置から送信された信号を受信する手順、復号化判断手段により復号化要求の有無を判断する手順、要求があれば、暗号化鍵復号化手段により第一の暗号化鍵の復号化を行う手順、復号化された該第一の暗号化鍵を用いて信号復号化手段により情報を復号化する手順、該情報を含む信号を信頼されないセッション制御サーバに送信する手順を、それぞれ実行させるためのセッション制御用プログラム。

【請求項 15】 セッション制御サーバがセッション確立中、あるいは、セッション変更中に得られた情報を元に NAT／ファイアウォール装置のフィルタリング条件を変更するセッション制御用プログラムであって、

セッション制御サーバのコンピュータに、通信装置の主情報通信経路の IP アドレスとポート番号を元に、NAT／ファイアウォール装置に対してフィルタリング条件の変更を要求する手順、不特定 IP アドレスから特定 IP アドレスおよびポート番号宛のパケットを通過させる手順、その後、他の通信装置から受信した暗号化情報を第一暗号化鍵を用いて復号化する手順、該通信装置の主情報通信経路の IP アドレスとポート番号を元に、NAT／ファイアウォール装置に対してフィルタリング条件の変更を要求する手順、特定 IP アドレスから特定 IP アドレスおよびポート番号宛のパケットを通過させる手順、その後、通信装置からメッセージの切断信号を受信する手順、NAT／ファイアウォール装置に対してフィルタリング条件の変更を要求する手順、指定 IP アドレスから指定 IP アドレスおよびポート番号宛のパケットを不通過とさせる手順を、それぞれ実行させるためのセッション制御用プログラム。

【請求項 16】 セッション制御サーバがセッション確立中、あるいは、セッション変更中に得られた情報を元に、暗号化された確情報について通信記録を可能にするセッション制御用プログラムであって、

セッション制御サーバのコンピュータに、通信装置の主情報通信経路の IP アドレスとポート番号を元に、NAT／ファイアウォール装置に対して、フィルタリング条件変更要求に加えて、主情報転送を指示する手順、該 NAT／ファイアウォール装置から主情報を受信する手順、取得済みの主情報暗号化の鍵情報を用いて主情報復号化手段により復号化を行う手順、復号化が終了すると、復号化さ

れた状態の主情報とその鍵情報を記録する手順を、それぞれ実行させるためのセッション制御用プログラム。

【請求項 17】 請求項 14 から 16 までのいずれかに記載のプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、信号の中継を行うセッション制御サーバ、暗号鍵に基づいて暗号化された通信を行う通信装置と通信システム、およびその通信方法、ならびにそのプログラムとそれを記録した記録媒体に関する。

【0002】

【従来の技術】

従来より、ユーザ間の通信情報の暗号化方式としては、IPSec (Security architecture for Internet Protocol)、TLS (Transport Layer Security)、S/MIME が挙げられる。

中継サーバが、情報を参照できる暗号化方式としては、IPSec、TLS がある。

IPSec は、TCP/IP の通信のセキュリティを強化するための技術であって、データを IP カプセル化してトンネリングする手法を規定する ESP (Encapsulation Secure Payload)、ユーザ認証用のデータを IP データに組み込む AH (Authentication Header) などがある。TLS は、バンキングシステムなど、クライアント・サーバ間のセキュリティが必要なアプリケーションで広く用いられる。

【0003】

IPSec、TLS の方法では、転送区間の始点、終点間で、暗号化鍵や方式の調整を行い、その結果に基づく暗号化通信を行い、通信装置が送受する伝達情報の機密性を向上させている。

上記に関しては、インターネットの標準化機関である IETF (Intern

et Engineering Task Force) がとりまとめている規格書の中で、RFC (Request for Comments) 3261 Section 26. 2 (非特許文献1 参照) がある。

【0004】

【非特許文献1】

RFC 3261 Section 26. 2

【0005】

【発明が解決しようとする課題】

IPSec や TLS などの暗号化方式では、転送区間の始点、終点間で暗号化方式、鍵の調整を行い、暗号化／復号化の処理を転送区間の始点、終点で行う必要があった。そのため、信号中継を行うセッション制御サーバで、必ず情報の復号化を行うことになり、セッション制御サーバに対する情報保護が可能な暗号化通信が困難であった。

また、S/MIME の暗号化方式では、発着通信装置間で暗号化を行い、全てのセッション制御サーバに対して情報保護が可能であるが、特定のセッション制御サーバに情報開示が必要な場合であっても、情報開示が不可能であるという問題点があった。

【0006】

(目的)

本発明の目的は、上記のような従来の課題を解決し、発着ユーザ間通信のエンド・エンド間の機密性を確保しながら、かつ、情報開示が必要な特定のセッション制御サーバに対してのみ情報開示を可能とするセッション制御サーバ、通信装置、通信システムおよび通信方法、ならびにそのプログラムと記録媒体を提供することにある。

【0007】

【課題を解決するための手段】

本発明は、

(1) 通信装置 A がセッション確立のための信号送信に先立ち、信号内の情報の暗号化のための第一の暗号化鍵 (対称暗号鍵) を生成する。

送信先の通信装置 B の第二の暗号化鍵（公開鍵あるいは事前共有鍵）と、通信装置 A がセッション確立に伴い情報を開示する対象である 0 以上のセッション制御サーバの第二の暗号化鍵（公開鍵あるいは事前共有鍵）を用いて、個々の第二の暗号化鍵毎に第一の暗号化鍵を暗号化する。

通信装置 A は、第一の暗号化鍵で暗号化した情報とともに、各第二の暗号化鍵（個々の公開鍵あるいは事前共有鍵）で暗号化した第一の暗号化鍵と、復号化要求指示をセッション制御サーバに送信する。

#### 【 0 0 0 8 】

なお、ここでの復号化要求指示は、通信装置 A がセッション確立に伴い情報を開示する対象であるセッション制御サーバを、セッション制御サーバを示す識別子の形で陽に提示していてもよいし、陽に提示していなくてもよい。

また、復号化対象のコンテンツ ID についても、陽に提示していてもよいし、陽に提示していなくてもよい。

陽に提示していない場合においては、例えばセッション確立に伴い経由される個々のセッション制御サーバにおいて、自らの保持する第二の暗号化鍵に対応する第二の復号化鍵による第一の暗号化鍵の復号化を行い、得られた情報が第一の暗号化鍵を示す表現形式に合致しているとき、自らを復号化要求を受けたセッション制御サーバと判断できるため、第二の暗号化鍵で暗号化された第一の暗号化鍵自身が復号化要求指示となる（請求項 1 参照）。

#### 【 0 0 0 9 】

（2）通信装置 A もしくは他のセッション管理サーバが送信した信号を受信したセッション制御サーバは、復号化要求有無、復号化対象の情報を判断し、復号化要求があった場合に、自らの第二の暗号化鍵に対応する第二の復号化鍵により第一の暗号化鍵の復号化を行う。もしくは、自らの第二の暗号化鍵に対応する第二の復号化鍵により第一の暗号化鍵の復号化を行い、その結果から復号化要求有無を判断する。または、これらのいずれをも行う。これらは、（1）記載の通信装置における復号化要求に依存する。

いずれの場合においても、得られた第一の暗号化鍵を用いて、暗号化情報の復号化を行う（請求項 2 参照）。

## 【0010】

(3) 上記(2)のセッション制御サーバは、更に暗号化した第一の暗号化鍵を、セッション単位に保管もしくは記憶する。その後、当該セッションの情報の復号化の際に再利用する(請求項3参照)。

(4) 通信装置Bは、暗号化した第一の暗号化鍵を添付した暗号化情報を含む信号を受信し、第一の暗号鍵の復号化を行い、その鍵を用いて、暗号化情報の復号化を行う。通信装置Bは、セッション単位に第一の暗号化鍵を保管もしくは記憶し、同一セッション内の情報の暗号化に、前記第一の暗号化鍵を再利用する。

第一の暗号化鍵を暗号化した情報が添付されない暗号化情報を含む信号を送信する。第一の暗号化鍵は、同一セッション内の情報の復号化にも再利用する(請求項4参照)。

## 【0011】

(5) 通信装置Aは、セッション単位に第一の暗号化鍵を保管もしくは記憶し、第一の暗号化鍵を暗号化した情報が添付されない暗号化情報を含む信号を受信した際に、同一セッション内の情報の復号化に、および、同一セッション内の情報の暗号化に、前記第一の暗号化鍵を再利用する(請求項5参照)。

(6) 通信装置Aおよび通信装置Bは、セッション内で、一定時間あるいは一定回数使用経過後、第一の暗号化鍵を更新し、更新信号とともに送信する(請求項6参照)。

(7) セッション制御サーバは、セッション内で通信装置A(あるいは通信装置B)より、第一の暗号化鍵の更新信号を受信すると、保管あるいは記憶していたそのセッションの第一の暗号化鍵を更新し、更新信号とともに通信装置B(あるいは通信装置A)に送信する(請求項7参照)。

## 【0012】

本発明においては、情報開示を行うセッション制御サーバを指定して、情報開示を行いながら安全な信号の送受信が可能となる。通信装置間の暗号化情報を含む信号通信の場合でも、特定のセッション制御サーバが信号情報の参照が可能となるため、その情報を基に通信制御が可能となることである。

## 【0013】

**【発明の実施の形態】**

以下、本発明の実施形態を、図面により詳細に説明する。

(システム構成)

図1は、本発明の実施形態に係る通信システムの構成図である。

図1に示すように、本通信システム100は、複数のセッション制御サーバ101と、複数の通信装置102とNAT/ファイアウォール装置103、およびネットワーク10を含むように構成される。

なお、通信装置102は、本発明による手順に従いセッション制御サーバ101を介して暗号化情報を含む信号により通信を行う。なお、通信システム100においては、セッション制御サーバ101は2台に限定されるものではない。ここでは、通信装置102が2台示されているが、2台に限定されるものではない。NAT/ファイアウォール装置103が1台示されているが、1台に限定されるものではない。

**【0014】**

なお、本発明によれば、通信装置102はパソコン、携帯端末、あるいはゲートウェイなどの通信機器を含み、ネットワーク10の構成は、有線、無線を問わない。以降は、説明の便宜を図るため、通信装置102-1を発信側とし、通信装置102-2を着信側として説明する。また、セッション制御サーバ101-1を発信側、セッション制御サーバ101-2を着信側として説明する。

通信装置102-1が暗号化情報とともに通信装置102-2用に暗号化した第一の暗号化鍵とセッション制御サーバ101-1用に暗号化した第一の暗号化鍵を、セッション制御サーバ101-1に送信する。

**【0015】**

セッション制御サーバ101-1が通信装置102-1から送信された暗号化情報と2つの暗号化した第一の暗号化鍵を受信し、これらのうちセッション制御サーバ用情報を復号化し、得られた第一の暗号化鍵で暗号化情報を復号化し、情報の参照が可能となる。

この際に、セッション制御サーバ101-1は、参照した情報をもとにNAT/ファイアウォール装置103に対して、フィルタリング条件の変更要求を送信

してもよい。NAT／ファイアウォール装置 103 からフィルタリング条件の変更完了通知を受信した後、セッション制御サーバ 101-1 は通信装置 102-1 から受信した暗号化情報を含む信号と 2 つの第一の暗号化鍵を、セッション制御サーバ 101-2 に送信する。

#### 【0016】

セッション制御サーバ 101-2 は、セッション制御サーバ 101-1 から送信された暗号化情報と 2 つの暗号化した第一の暗号化鍵を受信するが、これらを復号化できないため、暗号化された情報の参照はできない。セッション制御サーバ 101-2 は、受信した暗号化情報と 2 つの暗号化した第一の暗号化鍵を通信装置 102-2 に送信する。

通信装置 102-2 は、セッション制御サーバ 101-2 から受信した通信装置 102-2 用情報を復号化し、得られた第一の暗号化鍵で暗号化した情報を復号化することで、情報の参照が可能となる。

通信装置 102-2 は、通信装置 102-1 に送信すべき応答信号などの信号をセッション対応に記憶している第一の暗号化鍵を再利用して、暗号化し、セッション制御サーバ 101-1, 101-2 経由で、あるいは直接、通信装置 102-1 に送信する。

#### 【0017】

(通信装置)

図 3 は、本発明の実施形態に係る通信装置のブロック構成図である。

図 3 に示すように、通信装置 102 は、信号送信手段 120、セッション制御手段 121、暗号化鍵生成手段 122、暗号化鍵暗号化手段 123、信号情報暗号化手段 124、暗号化鍵再利用手段 125、信号情報復号化手段 126、暗号化鍵復号化手段 127、信号受信手段 128、暗号化鍵更新手段 129 を含むように構成される。

通信装置 102-1 は、セッション制御手段 121 で生成された信号のうち、機密性が必要な情報を、暗号化鍵生成手段 122 で生成された第一の暗号化鍵を使用して、信号暗号化手段 124 で暗号化する。

#### 【0018】



そして、その第一の暗号化鍵を、開示先通信装置およびサーバの第二の暗号化鍵（例えば、実施形態においては公開鍵とする）を使用して、暗号化鍵暗号化手段 123 により各々暗号化する。その際に、使用した第一の暗号化鍵は、暗号化鍵再利用手段 125 にてセッション識別子対応に保管もしくは記憶される。

セッション制御手段 121 で生成された情報のうち、暗号化していない情報に、セッション制御サーバ 101 および送信先通信装置に復号化を要求する情報を追加し、第一の暗号化鍵で暗号化した情報と、復号化要求対象が保持する第二の暗号化鍵により暗号化した第一の暗号化鍵とともに、信号送信手段 120 にて、セッション制御サーバ 101-1 に送信する。これにより、機密性が必要な情報について、特定のセッション制御サーバ 101-1 と通信装置 102-2 に対してのみ開示可能な状態で、信号送信が可能になる。

#### 【0019】

図 4 は、本発明の実施形態に係る通信装置 102-1 の送信信号例を示す図である。

通信装置 102-1 は、機密性が必要な情報を第一の暗号化鍵を使用して暗号化する。その第一の暗号化鍵を、開示先通信装置およびサーバの各々の第二の暗号化鍵を使用して各々暗号化する。暗号化していない情報に、セッション制御サーバ 101 に復号化要求する情報を追加する。第一の暗号化鍵で暗号化した情報と、復号化要求対象が保持する第二の暗号化鍵により暗号化した第一の暗号化鍵とともに、信号送信手段 120 にて、セッション制御サーバ 101-1 に送信する。

この送信信号例については、さらに、第 1 の実施形態の説明で図 6 とともに説明する。

#### 【0020】

図 5 は、本発明の実施形態に係る通信装置 102-2 の送信信号例を示す図である。

この送信信号例については、さらに、第 1 の実施形態の説明で、図 6 とともに説明する。

#### 【0021】

(セッション制御サーバ)

図 2 は、本発明の実施形態に係るセッション制御サーバのブロック構成図である。

図 2 に示すように、セッション制御サーバ 101 は、信号受信手段 110、復号化判断手段 111、暗号化鍵復号化手段 112、復号化鍵再利用手段 113、信号情報復号化手段 114、セッション制御手段 115、信号送信手段 116 を具備している。NAT/ファイヤウォール制御手段 117、主情報通信受信手段 118、主情報復号化手段 119 を具備している。

#### 【0022】

暗号化鍵復号化手段 112 は、第一の暗号化鍵の格納されたデータを見て、どの第二の暗号化鍵に対応した第二の復号化鍵を使用して、復号化するかを判断した上で、第一の暗号化鍵の復号化を行い、情報復号化手段 114 に復号化鍵を渡す。情報信号の復号化により、通信装置間の制御情報が参照可能となり、セッション制御手段 115 に必要な情報を提供する。

復号化鍵は、セッション制御手段 115 内の識別子に対応して、復号化鍵再利用手段 113 において、信号情報に含まれるセッションの識別子に対応して、復号化鍵を保管もしくは記憶する。

セッション制御手段 115 で信号送信の準備が整うと、信号受信手段 110 で受信した暗号化した情報と、暗号化した第一の暗号化鍵を含む信号を、信号送信手段 116 により通信装置 102-2 に送信する。

#### 【0023】

(第 1 の実施形態)

図 6 は、本発明の第 1 の実施形態に係る通信方法の説明図である。

第 1 の実施形態では、通信装置 102-1 で生成したセッション制御信号が、通信装置 102-1 から信頼されるセッション制御サーバ 101-1、信頼されないセッション制御サーバ 101-2 経由で通信装置 102-2 に送信される例を説明する。

例えば、図 4 に示すように、通信装置 102-1 からの送信信号は、RFC 3261 に準拠した SIP メッセージの 1 つである INVITE メソッド 400 で

あって、そのメッセージに含まれる通信装置間の制御情報（SDP：Session Description Protocol）405が暗号化されている。SDPには、通信装置102-1の主情報通信の情報として、受信用IPアドレス、ポート番号などを含む。改ざん防止のために、暗号化情報404に、通信装置102-1のユーザのデジタル署名を添付してもよい。

#### 【0024】

SIPメッセージは、セッション制御サーバ101-1、および、セッション制御サーバ101-2を経由して、通信装置102-2に送信されるものである。暗号化した情報は、S/MIMEのEnveloped-Data404として設定する。その暗号化に使用した鍵（第一の暗号化鍵）は、セッション制御サーバ101の公開鍵と、着ユーザの公開鍵（第二の暗号化鍵）とで各々暗号化し、Enveloped-Dataの中のRecipient Info406として設定する。

また、第一の暗号化鍵は、セッション制御サーバ101-1と通信装置102-1間の事前共有鍵や、通信装置102-1と通信装置102-2のユーザ間の事前共有鍵で、各々暗号化されてもよい。

#### 【0025】

そして、SIPメッセージ内の暗号化していない範囲401に、セッション制御サーバに復号化要求を示す値と、復号化すべきコンテンツIDとを含む。

改竄防止が必要なSIPメッセージ402に対して、通信装置102-1のユーザのデジタル署名403を添付してもよい。

セッション制御サーバ101-1は、通信装置102-1から送信されたINVITEメソッド400を信号受信手段110にて受信する。復号化判断手段111において、復号化要求パラメータ（例：Session-Policy）の値で、復号化要求を判断するか、暗号化された第一暗号化鍵が設定されたRecipient Info406の復号化可否で、復号化要求を判断してもよい。

#### 【0026】

復号化要求がある場合、暗号化鍵復号化手段112は、指定されたコンテンツIDの示すデータ404の中の、第一の暗号化鍵の格納されたデータ(Rec e

p i e n t I n f o) 4 0 6 の型を見て、どの第二の暗号化鍵に対応した第二の復号化鍵を使用して復号化するかを判断した上で、第一の暗号化鍵の復号化を行い、信号復号化手段 1 1 4 に復号化鍵を渡す。暗号化情報 4 0 5 の復号化により、通信装置間制御用の信号が参照可能となり、セッション制御手段 1 1 5 に必要な情報を提供する。

復号化要求がない場合や、指定されたコンテンツ ID が設定されていない場合は、復号化処理は行わない。

#### 【0027】

セッション制御サーバ 1 0 1 - 1 は、復号化要求の有無にかかわらず、セッション制御手段 1 1 5 において、通信装置 1 0 2 - 1 から受信した I N V I T E メソッドについて、処理（必要なパラメータ変更など）を行い、信号送信手段 1 1 6 よりセッション制御サーバ 1 0 1 - 2 に送信する。

セッション制御サーバ 1 0 1 - 2 は、セッション制御サーバ 1 0 1 - 1 から送信された I N V I T E メソッドを信号受信手段 1 1 0 にて受信する。

復号化判断手段 1 1 1 において、復号化要求パラメータ（例：S e s s i o n - P o l i c y）の値で復号化要求を判断するか、あるいは暗号化された第一暗号化鍵が設定された R e c e p i e n t I n f o 4 0 6 の復号化可否で、復号化要求を判断してもよい。

復号化要求がない、あるいは、復号化不可のため、暗号化された通信装置間の制御情報は参照できない。セッション制御手段 1 1 5 にて参照可能な情報をもとに、I N V I T E メソッドについて処理（必要なパラメータ変更など）を行い、信号送信手段 1 1 6 より通信装置 1 0 2 - 1 に送信する。

#### 【0028】

信号を受信した通信装置 1 0 2 - 2 は、信号受信手段 1 2 8 で受信した信号の情報が第一の暗号化鍵で暗号化されており、第一の暗号化鍵が暗号化されて添付されていると、自身の第二の暗号化鍵に対応する第二の復号化鍵（第一の暗号化鍵が公開鍵の場合は秘密鍵、あるいは第二の暗号化鍵が事前共有鍵であれば同事前共有鍵）を使用して、暗号化鍵復号化手段 1 2 7 で復号化し、第一の暗号化鍵を得る。その第一の暗号化鍵を使用して、暗号化された情報を信号復号化手段 1

26にて復号化し、情報が参照可能となる。その情報をセッション制御手段121に提示する。

#### 【0029】

セッション制御手段121は、必要に応じて送信すべき情報を生成するとともに、暗号鍵を暗号化鍵再利用手段125にてセッション識別子対応に保管する。

例えば、図5に示すようなINVITEメソッドに対する応答信号として200 OK 500を送信する。送信すべき情報について、保管もしくは記憶している第一の暗号化鍵を使用して、信号暗号化手段124にて暗号化した情報505をEncrypted-Dataとして設定し、信号送信手段120より信号を送信する。

また、改ざん防止のために、暗号化した情報504に対してデジタル署名を添付してもよい。

#### 【0030】

(応用例1：請求項6参照)

その後のセッションの継続信号が、例えばMESSAGEメソッドが通信装置102-1よりセッション制御サーバ101-1, 101-2経由で通信装置102-2に送信される。通信装置102-1は、セッション単位に保管または記録している第一暗号化鍵を使用して、MESSAGEメソッドに設定するインスタントメッセージの内容を暗号化する。第一暗号化鍵を添付しないで、暗号化した情報を含むMESSAGEメソッドを送信する。

当該信号を受信した通信装置102-2は、暗号化鍵再利用手段123において、セッション識別子をキーに保管している第一暗号化鍵を取得し、その第一暗号化鍵にて暗号化情報を復号化する。

#### 【0031】

(応用例2：請求項3参照)

セッション制御サーバ101-1においても、セッション単位に保管している第一の暗号化鍵を使用して暗号化情報を復号化する。

#### 【0032】

(応用例3：請求項6参照)

また、一定時間経過後、通信装置 102-1 が MESSAGE メソッドをセッション制御サーバ 101-1, 101-2 経由で通信装置 102-2 に送信する際に、暗号化鍵更新手段 129 にて第一暗号化鍵を更新する。更新した暗号化鍵を用いて情報を暗号化し、S/MIME の Enveloped-Data として設定する。

その暗号化に使用した鍵（更新した第一の暗号化鍵）は、セッション制御サーバの公開鍵と、着ユーザの公開鍵（第二の暗号化鍵群）とで各々暗号化し、Enveloped-Data の中の Recipient Info として設定する。

更新した第一の暗号化鍵を添付した暗号化情報を含む信号を受信した通信装置 102-2 は、更新された第一の暗号化鍵を暗号化鍵再利用手段 125 にて保管あるいは記憶する。

### 【0033】

（応用例 4：請求項 7 参照）

更新した第一の暗号化鍵を添付した暗号化情報を含む信号を受信したセッション制御サーバ 101-1 は、更新された第一の暗号化鍵を暗号化鍵再利用手段 113 にて保管あるいは記憶する。

### 【0034】

（第 2 の実施形態）

図 7 は、本発明の第 2 の実施形態に係る通信方法の説明図である。

ここでは、セッション制御サーバが、セッション確立中に得られた情報を元に NAT/ファイアウォール装置 103 のフィルタリング条件を変更する例を示している。

例えば、セッション制御サーバが、通信装置 102-1 から受信した信号が RFC 3261 に準拠した SIP メッセージの 1 つである INVITE メソッドであって、そのメッセージに含まれる通信装置間の制御情報（SDP: Session Description Protocol）が暗号化されている。

第二の暗号化鍵に対応する第二の復号化鍵を使用して復号化することにより、制御情報に設定されている通信装置 102-1 の主情報通信径路の IP アドレスとポート番号などが参照可能となる。この情報を元に、NAT/ファイアウォー

ル制御手段 117 において、遠隔の NAT/ファイアウォール装置 103 に対してフィルタリング条件の変更（不特定 IP アドレスから特定 IP アドレス+ポート番号宛のパケット通過指示）を要求する。

#### 【0035】

その後、通信装置 102-2 から受信した信号が、SIP メッセージの 1 つである 200 OK 応答であって、そのメッセージに含まれる通信装置間の制御情報（SDP）が暗号化されている。復号化鍵再利用手段 113 に記憶していた第一の暗号化鍵を用いて暗号化情報を復号化して、通信装置 102-2 の主情報通信径路の IP アドレスとポート番号が通信装置間の制御情報が参照可能となる。この情報を元に、NAT/ファイアウォール制御手段 117 において、遠隔の NAT/ファイアウォール装置 103 に対してフィルタリング条件の変更（特定 IP アドレスから特定 IP アドレス+ポート番号宛のパケット通過指示）を要求する。これにより、NAT/ファイアウォール装置 103 において、通信装置 102-1 と通信装置 102-2 間の主情報についてパケット通過が可能となる。

#### 【0036】

その後、通信装置 102-1 あるいは 102-2 から送信した SIP メッセージの切断信号である BYE メソッドを受信すると、セッション制御サーバ 101-1 は、NAT/ファイアウォール制御手段 117 において、NAT/ファイアウォール装置 103 に対してフィルタリング条件の変更（指定 IP アドレスから指定 IP アドレス+ポート番号宛のパケット不通過指示）を要求する。

本実施形態で示したように、通信装置より信号内の情報を安全に開示されたセッション制御サーバ 101-1 により、セッション単位に NAT/ファイアウォール制御を行うことができるので、アクセス制御の精度を高めることが可能となる。情報を開示されないセッション制御サーバ 101-2 は、主情報の経路情報が参照できないため、主情報のモニタが困難となり、その結果、主情報通信の機密性を高めることができる。

#### 【0037】

（第 3 の実施形態）

図 8 は、本発明の第 3 の実施形態に係る通信方法の説明図である。

ここでは、セッション制御サーバ101-1が、セッション確立中に得られた情報を元に、暗号化された主情報についても、通信記録が可能となる例を説明する。

例えば、通信装置102-1からの送信信号は、RFC3261に準拠したSIPメッセージの1つであるINVITEメソッドであって、そのメッセージに含まれる通信装置情報SDPが暗号化されている。SDPには、通信装置102-1、通信装置102-2間に主情報通信の際に使用するIPアドレス、ポート番号に加えて、主情報暗号化のための鍵情報を含む。

セッション制御サーバ101-1が、主情報通信記録の手段（受信手段118）と、主情報復号化手段119を備え、遠隔のNAT/ファイアウォール装置103に対して指示を送信する。

#### 【0038】

この指示は、前述の第2の実施形態で説明したフィルタリング条件変更要求に加えて、主情報転送を指示する。セッション制御サーバ101-1の主情報通信受信手段118にて、NAT/ファイアウォール装置103から主情報を受信する。主情報が暗号化されている場合、既に取得済みの主情報暗号化の鍵情報を用いて、主情報復号化手段119にて復号化を行う。

復号化が正常終了すると、復号化された主情報、あるいは、暗号化した状態の主情報とその鍵情報を記録する。

セッション制御サーバ101-2は、暗号化情報を復号化できないため、通信装置情報SDPは参照できず、SDPに含まれる主情報暗号化のための鍵情報は参照できない。そのため、ネットワーク内のモニタ装置で主情報をモニタしても、暗号化されており、それを復号化することができない。

このように、主情報が暗号化されている場合でも、セッション制御サーバによる復号化した主情報の記録が行えるため、通信情報の監査、および、記録が可能となる。

#### 【0039】

なお、第1の実施形態、第2の実施形態および第3の実施形態で説明した処理順序をプログラム化して、CD-ROMなどの記録媒体に格納しておけば、プロ



グラムの販売や貸与の際に便利であり、また、セッション制御サーバ 101-1, 101-2 のコンピュータに記録媒体を装着して、プログラムをインストールし、これを実行させることで、本発明を容易に実現することができる。

#### 【0040】

このように、本実施形態に係る通信システムは、通信装置間だけでなく、信号中継を行うセッション制御サーバに対しても、情報開示が可能であるため、通信装置が送受信する伝達信号の機密性を高めながら、特定のセッション制御サーバによる通信制御が可能となる。

#### 【0041】

##### 【発明の効果】

以上説明したように、本発明によれば、通信装置間の機密性の高い信号送受信を保証した上で、通信装置の要求に応じて特定のセッション制御サーバのみ、信号情報を開示することが可能である。また、通信装置間の接続構成によらず、信号情報を開示するセッション制御サーバの指定が可能となる。

##### 【図面の簡単な説明】

##### 【図1】

本発明の実施形態に係る通信システムのブロック構成図である。

##### 【図2】

図1におけるセッション制御サーバの詳細な構成図である。

##### 【図3】

図1における通信装置の詳細な構成図である。

##### 【図4】

本発明の実施形態に係る通信装置 102-1 の送信信号例を示す図である。

##### 【図5】

本発明の実施形態に係る通信装置 102-2 の送信信号例を示す図である。

##### 【図6】

本発明の第1の実施形態に係る通信方法の説明図である。

##### 【図7】

本発明の第2の実施形態に係る通信方法の説明図である。

## 【図 8】

本発明の第 3 の実施形態に係る通信方法の説明図である。

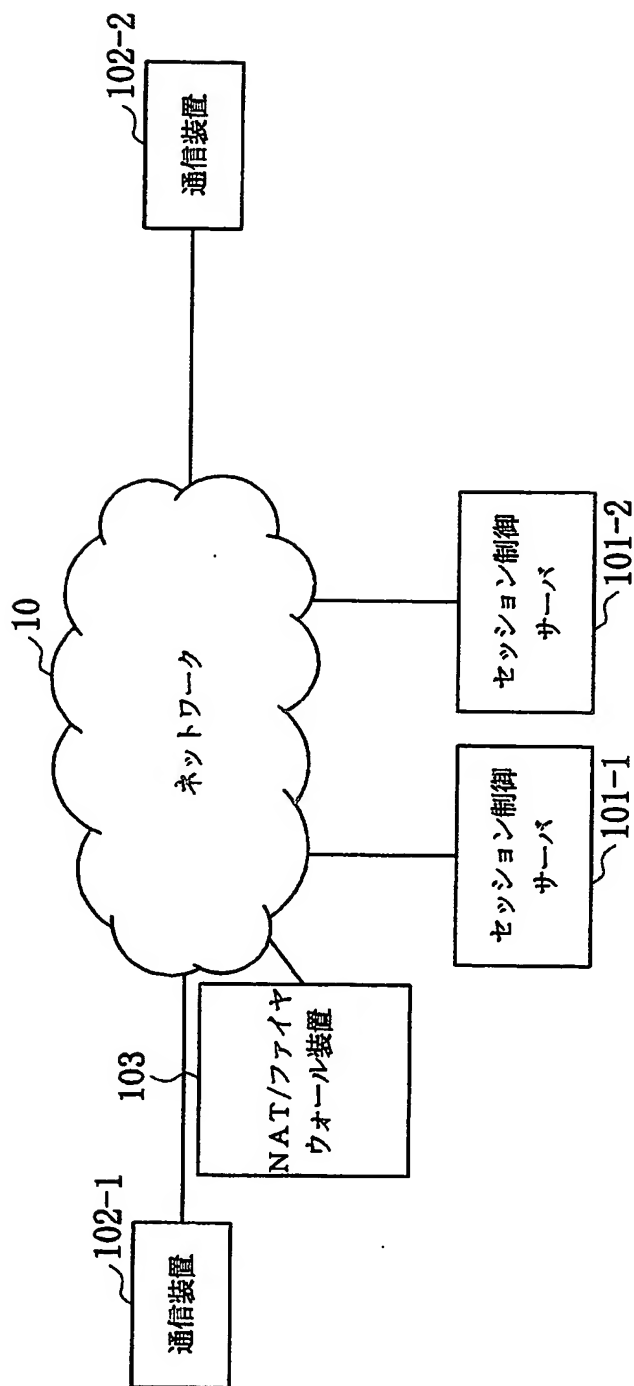
## 【符号の説明】

10…ネットワーク、101-1, 101-2…セッション制御サーバ、  
102-1, 102-2…通信装置、110…信号受信手段、  
111…復号化判断手段、112…暗号化鍵復号化手段、  
113…復号化鍵再利用手段、114…信号復号化手段、  
115…セッション制御手段、116…信号送信手段、  
117…NAT/ファイアウォール制御手段、118…主情報通信受信手段、  
119…主情報復号化手段、120…信号送信手段、  
121…セッション制御手段、122…暗号化鍵生成手段、  
123…暗号化鍵暗号化手段、124…信号暗号化手段、  
125…暗号化鍵再利用手段、126…信号復号化手段、  
127…暗号化鍵復号化手段、128…信号受信手段、  
129…暗号化鍵更新手段、  
400～406…通信装置 102-1 の送信信号領域、  
500～505…通信装置 102-2 の送信信号領域。

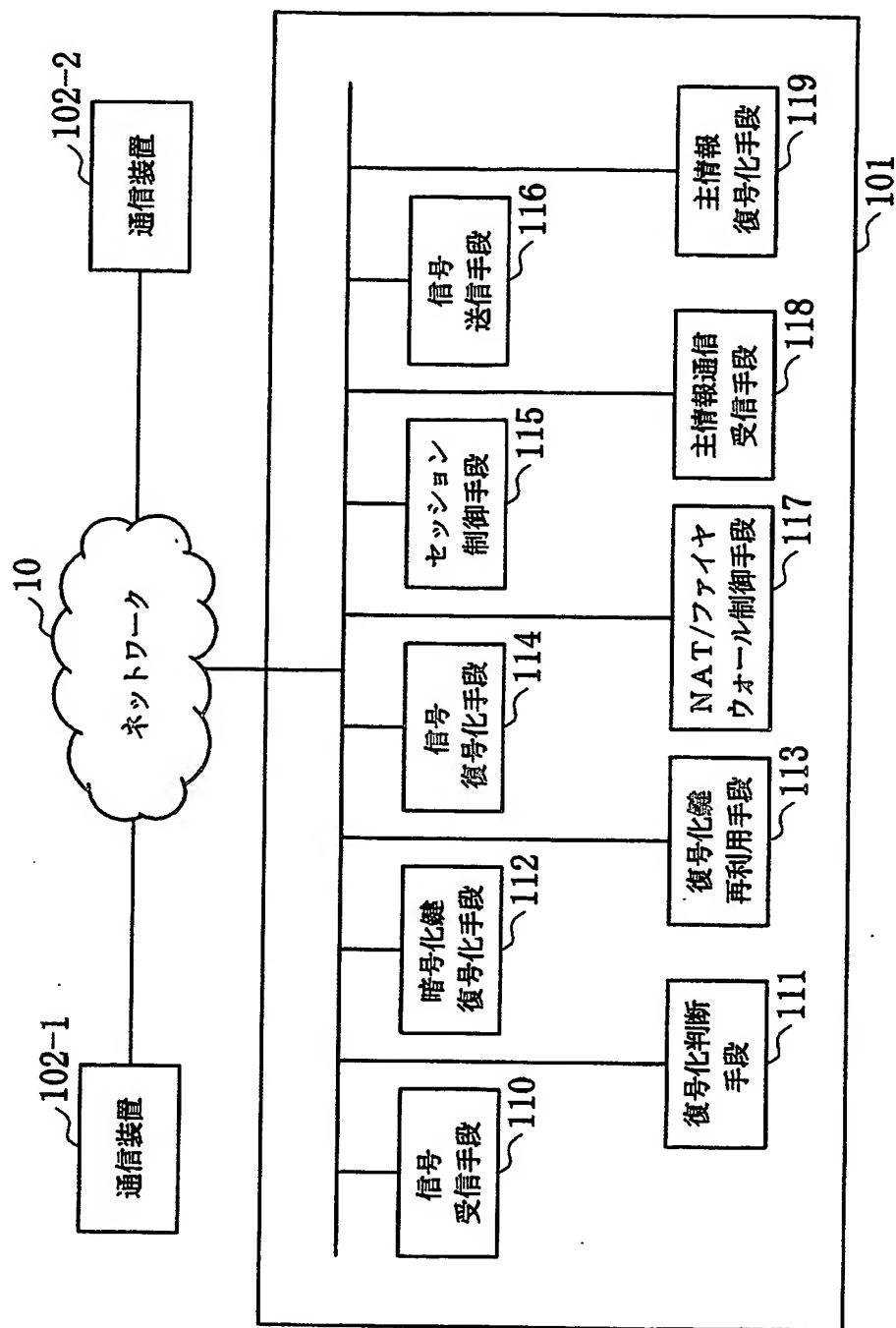
【書類名】 図面

【図 1】

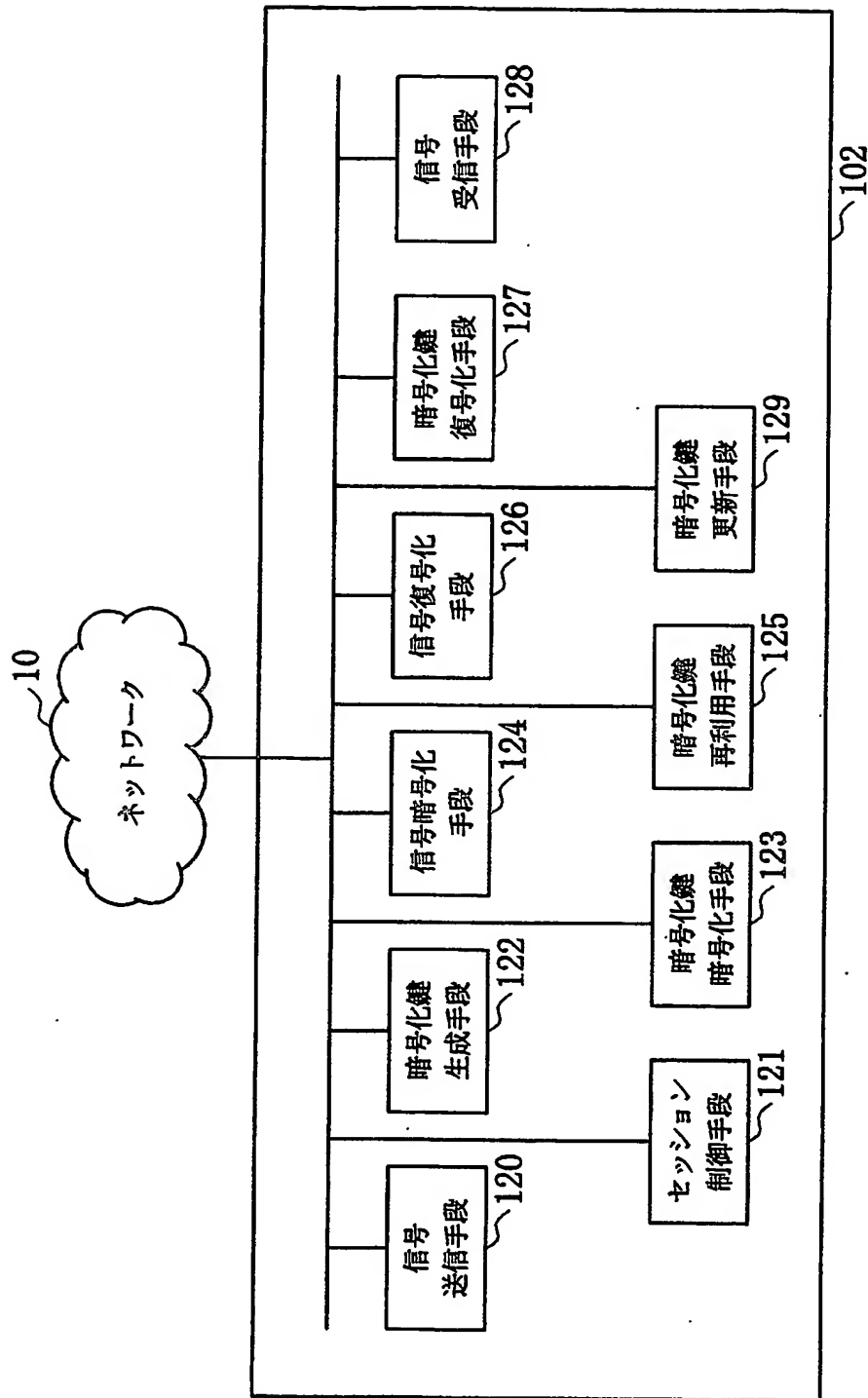
100



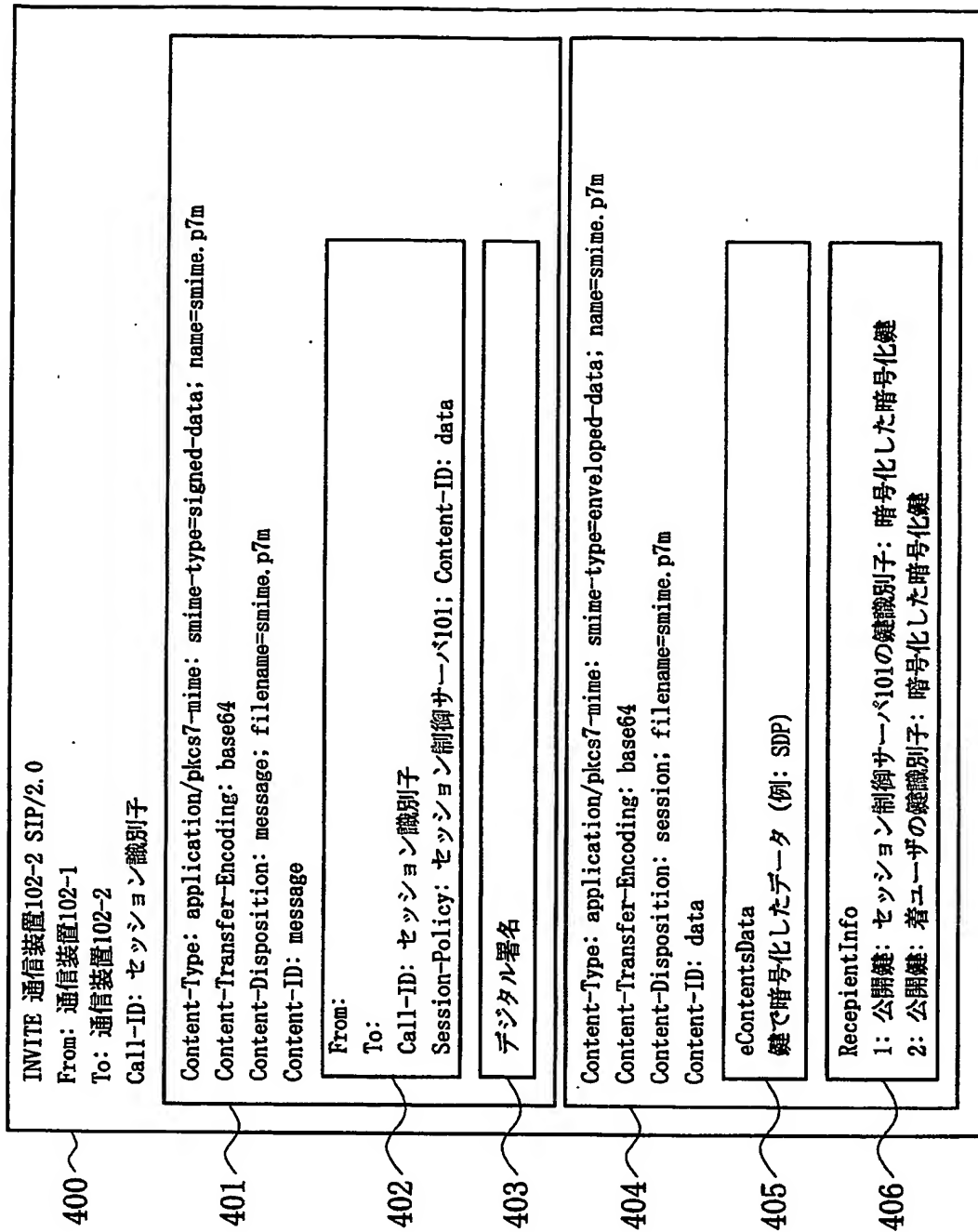
【図 2】



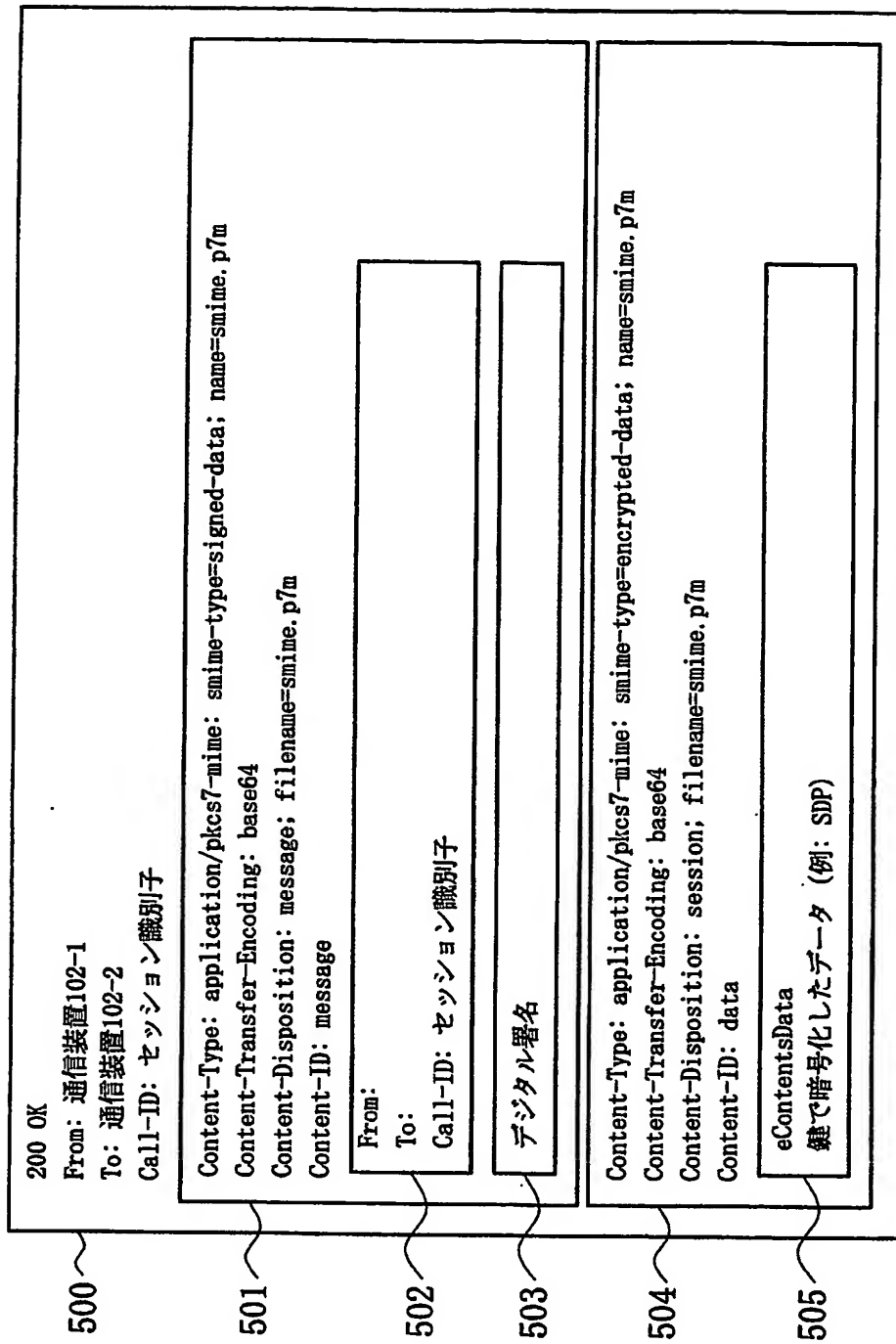
【図 3】



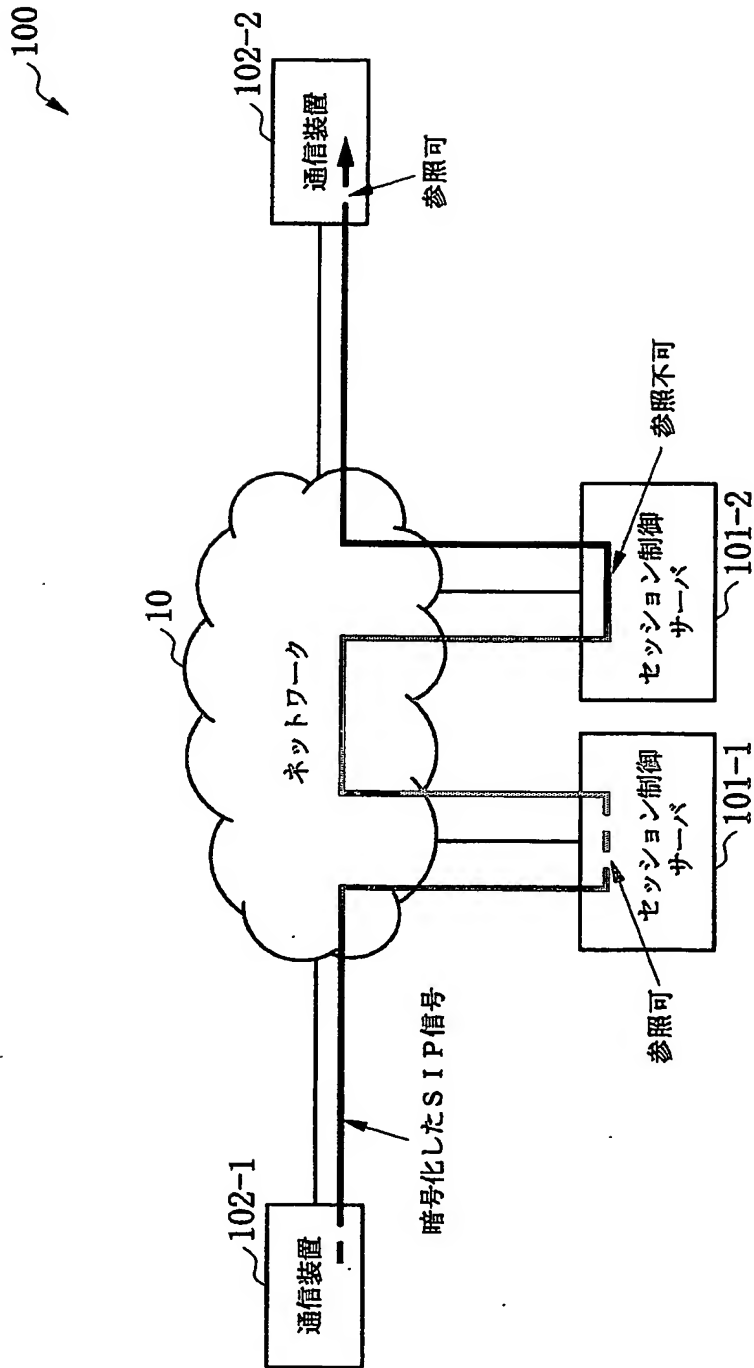
【図 4】



【図 5】

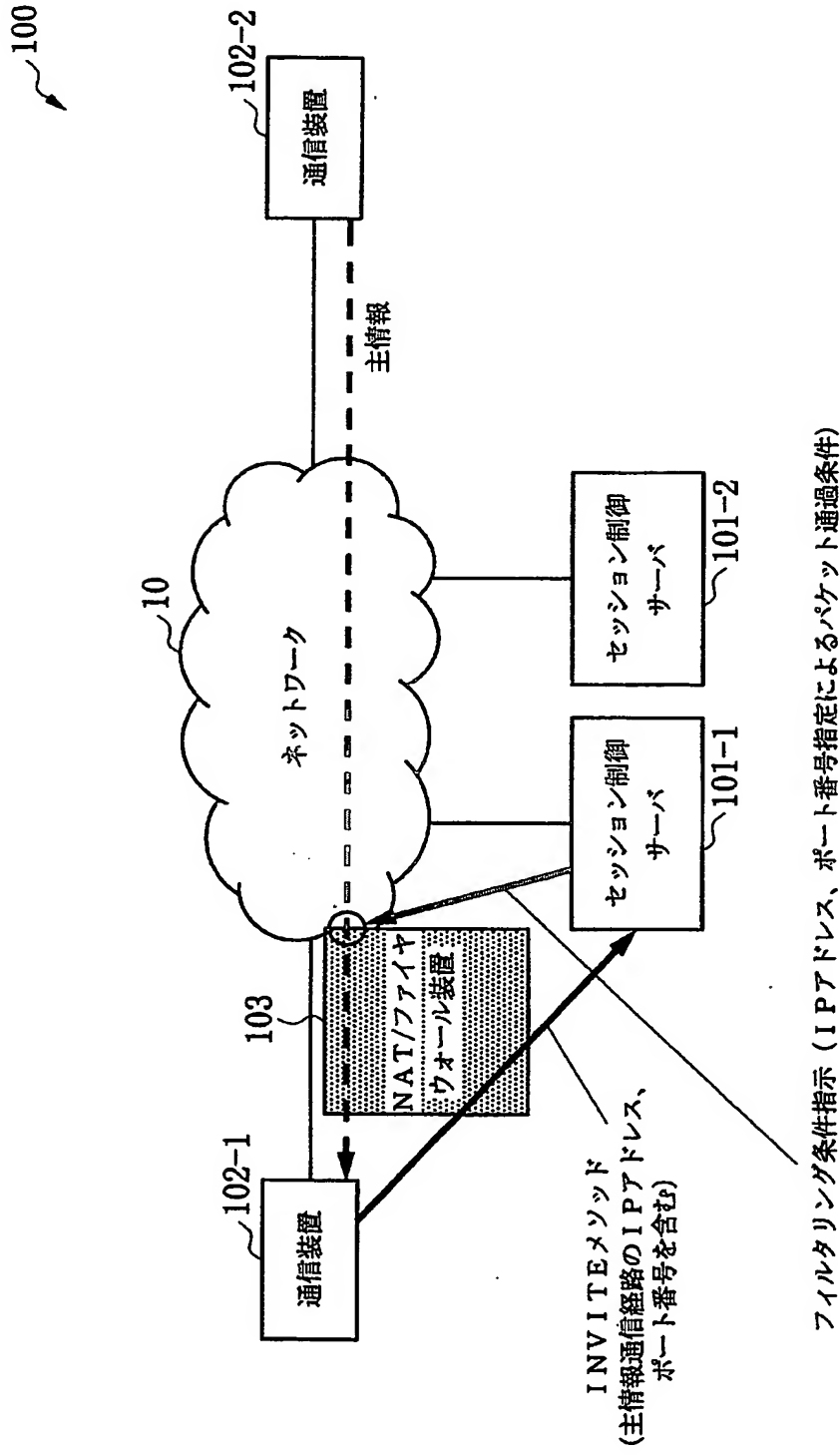


【図6】

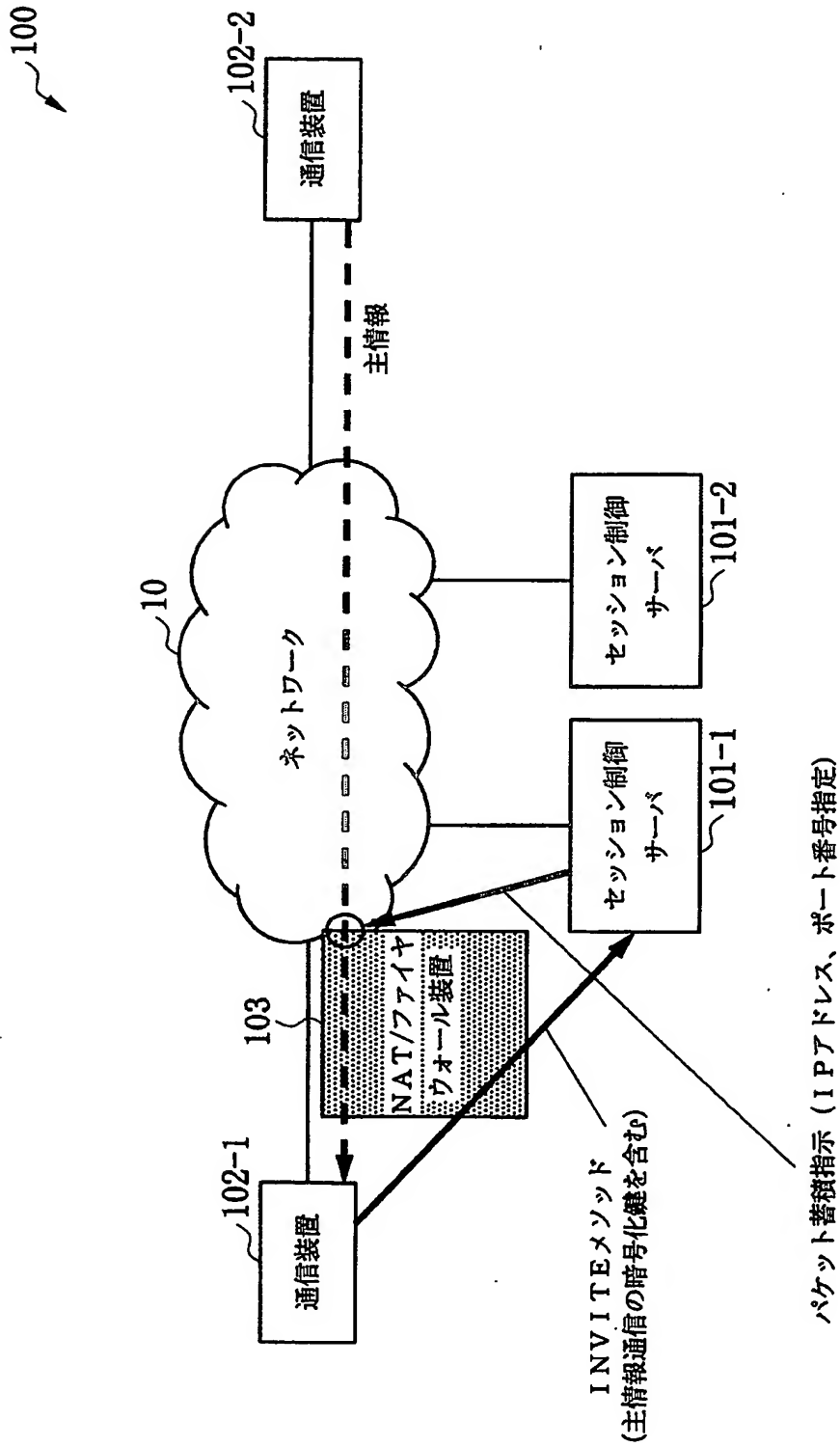




【図7】



【図8】



【書類名】

要約書

【要約】

【課題】 発着通信端末間の暗号化通信を提供し、かつ特定のセッション制御サーバに対してのみ情報開示を可能とする。

【解決手段】 通信装置 102-1, 102-2 が、情報開示したい特定の中継サーバ 101-1、または 101-2 の公開鍵で暗号化した情報暗号化鍵を、情報公開鍵で暗号化した情報とともに送信する。また、情報暗号化鍵の暗号化に使用する鍵は、公開鍵の代わりに事前共有鍵も使用可能である。これにより、通信端末で暗号化した情報を選択的にサーバ毎に復号可・不可を制御することが可能となる。

【選択図】

図 1

認定・付加情報

|         |                |
|---------|----------------|
| 特許出願の番号 | 特願 2003-176568 |
| 受付番号    | 50301034193    |
| 書類名     | 特許願            |
| 担当官     | 第八担当上席 0097    |
| 作成日     | 平成15年 6月23日    |

<認定情報・付加情報>

|       |             |
|-------|-------------|
| 【提出日】 | 平成15年 6月20日 |
|-------|-------------|

次頁無

出 願 人 履 歴 情 報

識別番号

[000004226]

1. 変更年月日  
[変更理由]  
住 所  
氏 名

1999年 7月15日  
住所変更  
東京都千代田区大手町二丁目3番1号  
日本電信電話株式会社

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

☒ **BLACK BORDERS**

☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**

☐ **FADED TEXT OR DRAWING**

☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**

☐ **SKEWED/SLANTED IMAGES**

☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**

☐ **GRAY SCALE DOCUMENTS**

☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**

☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**

☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**